

EXHIBIT 5

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability
<p>A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:</p> <p>receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;</p>	<p>Trend Micro Apex Central includes <i>a non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive first vulnerability information</i> (e.g., a smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof, including associated information including but not limited to information describing the actual vulnerabilities themselves, information describing endpoints that contain the particular operating system/application/version thereof, information describing policy/detection/remediation techniques for addressing the actual vulnerabilities relevant to the particular operating system/application/version thereof including signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) <i>from at least one first data storage</i> (e.g., memory on the at least one device storing a repository of the smaller “sub-set of actual vulnerabilities relevant to a particular operating system/application/version thereof, etc.) <i>that is generated utilizing second vulnerability information</i> (e.g., a larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof, including associated information including but not limited to information describing the possible vulnerabilities themselves, information describing the different operating systems/applications/versions thereof, information describing policy/detection/remediation techniques for addressing the potential vulnerabilities relevant to the different operating systems/applications/versions thereof including signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) <i>from at least one second data storage</i> (e.g., Common Vulnerabilities and Exposures (CVE) database, etc.) <i>that is used to identify a plurality of potential vulnerabilities</i> (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.);</p> <p>Note: See, for example, the evidence below (emphasis added, if any):</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability												
	<p>“About the Web Console</p> <p>The Apex Central web console provides centralized management, monitoring, and security visibility for all endpoints and users protected by Trend Micro products registered to the Apex Central server. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. <u>The web console lets you administer the Apex Central network from any machine using a compatible web browser.</u></p> <p>Apex Central supports the following web browsers:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer™ 11 • Microsoft Edge™ • Google Chrome™ <p>Web Console Requirements</p> <table> <tr> <th>Resource</th><th>Requirement</th></tr> <tr> <td>Processor</td><td>300 MHz Intel™ Pentium™ processor or equivalent</td></tr> <tr> <td>RAM</td><td>128 MB minimum</td></tr> <tr> <td>Available disk space</td><td>30 MB minimum</td></tr> <tr> <td>Browser</td><td>Microsoft Internet Explorer™ 11, Microsoft Edge™, or Google Chrome™</td></tr> <tr> <td></td><td>Important: When using Internet Explorer to access the Apex Central web console, turn off Compatibility View.</td></tr> </table> <p><i>Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 2-2 to 2-3</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>	Resource	Requirement	Processor	300 MHz Intel™ Pentium™ processor or equivalent	RAM	128 MB minimum	Available disk space	30 MB minimum	Browser	Microsoft Internet Explorer™ 11, Microsoft Edge™, or Google Chrome™		Important: When using Internet Explorer to access the Apex Central web console, turn off Compatibility View.
Resource	Requirement												
Processor	300 MHz Intel™ Pentium™ processor or equivalent												
RAM	128 MB minimum												
Available disk space	30 MB minimum												
Browser	Microsoft Internet Explorer™ 11, Microsoft Edge™, or Google Chrome™												
	Important: When using Internet Explorer to access the Apex Central web console, turn off Compatibility View.												

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability																										
	<p>“Attack Discovery Detection Information</p> <p><u>Provides general information about threats detected by Attack Discovery</u></p> <table> <tr> <th>Data</th><th>Description</th></tr> <tr> <td>Generated</td><td>The date and time the managed product generated the data</td></tr> <tr> <td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr> <tr> <td>Endpoint</td><td>The name of the endpoint</td></tr> <tr> <td>Product</td><td>The name of the managed product or service</td></tr> <tr> <td>Managing Server Entity</td><td>The display name of the managed product server in Apex Central to which the endpoint reports</td></tr> <tr> <td>Product Version</td><td>The version of the managed product</td></tr> <tr> <td>Endpoint IP</td><td>The IP address of the endpoint</td></tr> <tr> <td>Risk Level</td><td>The risk level assigned by Attack Discovery</td></tr> <tr> <td>Pattern Version</td><td>The Attack Discovery pattern number for the detection type</td></tr> <tr> <td>Rule ID</td><td>The serial number of the detection rule</td></tr> <tr> <td>Rule Name</td><td>The rules which specify behaviors to be detected by Attack Discovery</td></tr> <tr> <td>Related Objects</td><td> <p>The number of detections</p> <p>Click the count to view additional details.</p> <p>For more information, see Detailed Attack Discovery Detection Information on page B-11.</p> </td></tr> </table>	Data	Description	Generated	The date and time the managed product generated the data	Received	The date and time Apex Central received the data from the managed product	Endpoint	The name of the endpoint	Product	The name of the managed product or service	Managing Server Entity	The display name of the managed product server in Apex Central to which the endpoint reports	Product Version	The version of the managed product	Endpoint IP	The IP address of the endpoint	Risk Level	The risk level assigned by Attack Discovery	Pattern Version	The Attack Discovery pattern number for the detection type	Rule ID	The serial number of the detection rule	Rule Name	The rules which specify behaviors to be detected by Attack Discovery	Related Objects	<p>The number of detections</p> <p>Click the count to view additional details.</p> <p>For more information, see Detailed Attack Discovery Detection Information on page B-11.</p>
Data	Description																										
Generated	The date and time the managed product generated the data																										
Received	The date and time Apex Central received the data from the managed product																										
Endpoint	The name of the endpoint																										
Product	The name of the managed product or service																										
Managing Server Entity	The display name of the managed product server in Apex Central to which the endpoint reports																										
Product Version	The version of the managed product																										
Endpoint IP	The IP address of the endpoint																										
Risk Level	The risk level assigned by Attack Discovery																										
Pattern Version	The Attack Discovery pattern number for the detection type																										
Rule ID	The serial number of the detection rule																										
Rule Name	The rules which specify behaviors to be detected by Attack Discovery																										
Related Objects	<p>The number of detections</p> <p>Click the count to view additional details.</p> <p>For more information, see Detailed Attack Discovery Detection Information on page B-11.</p>																										

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability	
	Generated (Local Time)	<p>The time in the agent's local timezone when Attack Discovery detected the threat</p> <p>The time is displayed with the UTC offset.</p>
	Instance ID	<p>The detection ID assigned to the event</p> <p>Entries having the same instance ID belong under the same event.</p>
	Tactics	<p>The MITRE ATT&CK™ tactic(s) detected</p> <p>For more information, see https://attack.mitre.org/tactics/enterprise/.</p>
	Techniques	<p>The MITRE ATT&CK™ technique(s) detected</p> <p>For more information, see https://attack.mitre.org/techniques/enterprise/.</p>
<p><i>Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-10</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf</p> <p>“Threat Encyclopedia</p> <p>Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. <u>The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.</u></p>		

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability
	<p>Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:</p> <ul style="list-style-type: none"> • Malware and malicious mobile code currently active or "in the wild" • Correlated threat information pages to form a complete web attack story • Internet threat advisories about targeted attacks and security threats • Web attack and online trend information • Weekly malware reports" <p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 25-2 to 25-3 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>"Understanding the Apex Central Database</p> <p><u>Apex Central uses the Microsoft SQL Server database (db_ApexCentral.mdf) to store data included in logs, Communicator schedule, memory on the at least one device, user account, network environment, and notification settings.</u></p> <p>The Apex Central server establishes the database connection using a System DSN ODBC connection. The Apex Central installation generates this connection as well as the ID and password used to access db_ApexCentral.mdf. The default ID is sa. Apex Central encrypts the password.</p> <p>To maximize the SQL server security, configure any SQL account used to manage db_ApexCentral with the following minimum permissions:</p> <ul style="list-style-type: none"> • dbcreator for the server role • db_owner role for db_ApexCentral

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability
	<p><u>Logs from managed products contribute to database expansion.</u> Managed products send various log types to Apex Central.”</p> <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 23-2 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>
<p>said first vulnerability information generated utilizing the second vulnerability information, by:</p> <p>identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and</p>	<p>Trend Micro Apex Central includes <i>said first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>generated utilizing the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof), <i>by: identifying at least one configuration</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>associated with a plurality of devices</i> (e.g., managed products and endpoints, etc.) <i>including a first device, a second device, and a third device</i> (e.g., a first, second, and third of the managed products and endpoints, etc.), <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Vulnerability attack</p> <p>Malware or hacker attacks that <u>exploits a security weakness typically found in programs and operating systems.</u>”</p> <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 3-10 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“Procedure</p> <ol style="list-style-type: none"> 1. Go to Administration > Security Agent Download. 2. Select the operating system.

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability
	<ul style="list-style-type: none"> • Windows 64-bit: Select to create a 64-bit MSI installation package for Apex One Security Agents • Windows 32-bit: Select to create a 32-bit MSI installation package for Apex One Security Agents • Mac OS: Select to create a ZIP installation package for Apex One (Mac) Security Agents” <i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 9-3 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) <p>“About Apex Central</p> <p>Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. <u>Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints.</u> The Apex Central web-based management console <u>provides a single monitoring point for antivirus and content security products and services throughout the network.</u> Apex Central enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy components, such as antivirus pattern files, scan engines, and antispam rules, throughout the network to ensure up-to-date protection. Apex Central allows both manual and pre-scheduled updates, and allows the configuration and administration of products as groups or as individuals for added flexibility.” <i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 1-2 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>
determining that the plurality of devices is actually vulnerable to at least one actual vulnerability	Trend Micro Apex Central includes <i>determining that the plurality of devices (e.g., managed products and endpoints, etc.) is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability												
based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;	<p>Mac OS, or an application/version thereof, etc.), <i>utilizing the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is used to identify the plurality of potential vulnerabilities</i> (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“The Threat Type column displays the following threat types.</p> <table data-bbox="661 769 1906 1354"> <tr> <th data-bbox="661 769 1010 810">Threat Type</th><th data-bbox="1016 769 1906 810">Description</th></tr> <tr> <td data-bbox="661 810 1010 891">Ransomware</td><td data-bbox="1016 810 1906 891">Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr> <tr> <td data-bbox="661 891 1010 1045">Known Advanced Persistent Threat (APT)</td><td data-bbox="1016 891 1906 1045">Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</td></tr> <tr> <td data-bbox="661 1045 1010 1127">Social engineering attack</td><td data-bbox="1016 1045 1906 1127">Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr> <tr> <td data-bbox="661 1127 1010 1208">Vulnerability attack</td><td data-bbox="1016 1127 1906 1208">Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr> <tr> <td data-bbox="661 1208 1010 1354">Lateral movement</td><td data-bbox="1016 1208 1906 1354">Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr> </table>	Threat Type	Description	Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid	Known Advanced Persistent Threat (APT)	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents	Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file	Vulnerability attack	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems	Lateral movement	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
Threat Type	Description												
Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid												
Known Advanced Persistent Threat (APT)	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents												
Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file												
Vulnerability attack	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems												
Lateral movement	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system												

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability							
	Unknown threats	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer						
	C&C callback	Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware						
	Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)							
identify an occurrence in connection with at least one of the plurality of devices;	<p>Trend Micro Apex Central is configured to <i>identify an occurrence</i> (e.g., a positively-identified attack based on one of the known threat types, etc.) <i>in connection with at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“The Threat Type column displays the following threat types.</p> <table><tr><th>Threat Type</th><th>Description</th></tr><tr><td><u>Ransomware</u></td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr><tr><td><u>Known Advanced Persistent Threat (APT)</u></td><td>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</td></tr></table>		Threat Type	Description	<u>Ransomware</u>	Malware that prevents or limits users from accessing their system unless a ransom is paid	<u>Known Advanced Persistent Threat (APT)</u>	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents
Threat Type	Description							
<u>Ransomware</u>	Malware that prevents or limits users from accessing their system unless a ransom is paid							
<u>Known Advanced Persistent Threat (APT)</u>	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents							

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability	
	<u>Social engineering attack</u>	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file
	<u>Vulnerability attack</u>	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems
	<u>Lateral movement</u>	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
	<u>Unknown threats</u>	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer
	<u>C&C callback</u>	Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware
	Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)	
determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices,	Trend Micro Apex Central is configured to <i>determine that the at least one actual vulnerability of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.) <i>is susceptible to being taken advantage of by the occurrence</i> (e.g., the positively-identified attack based on one of the known threat types, etc.) <i>identified in connection with the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.), <i>utilizing the first vulnerability information</i> (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof); and	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability																										
utilizing the first vulnerability information; and	<p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Attack Discovery Detection Information</p> <p><u>Provides general information about threats detected by Attack Discovery</u></p> <table> <tr> <th>Data</th><th>Description</th></tr> <tr> <td>Generated</td><td>The date and time the managed product generated the data</td></tr> <tr> <td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr> <tr> <td>Endpoint</td><td>The name of the endpoint</td></tr> <tr> <td>Product</td><td>The name of the managed product or service</td></tr> <tr> <td>Managing Server Entity</td><td>The display name of the managed product server in Apex Central to which the endpoint reports</td></tr> <tr> <td>Product Version</td><td>The version of the managed product</td></tr> <tr> <td>Endpoint IP</td><td>The IP address of the endpoint</td></tr> <tr> <td>Risk Level</td><td>The risk level assigned by Attack Discovery</td></tr> <tr> <td>Pattern Version</td><td>The Attack Discovery pattern number for the detection type</td></tr> <tr> <td>Rule ID</td><td>The serial number of the detection rule</td></tr> <tr> <td>Rule Name</td><td>The rules which specify behaviors to be detected by Attack Discovery</td></tr> <tr> <td>Related Objects</td><td> The number of detections Click the count to view additional details. </td></tr> </table>	Data	Description	Generated	The date and time the managed product generated the data	Received	The date and time Apex Central received the data from the managed product	Endpoint	The name of the endpoint	Product	The name of the managed product or service	Managing Server Entity	The display name of the managed product server in Apex Central to which the endpoint reports	Product Version	The version of the managed product	Endpoint IP	The IP address of the endpoint	Risk Level	The risk level assigned by Attack Discovery	Pattern Version	The Attack Discovery pattern number for the detection type	Rule ID	The serial number of the detection rule	Rule Name	The rules which specify behaviors to be detected by Attack Discovery	Related Objects	The number of detections Click the count to view additional details.
Data	Description																										
Generated	The date and time the managed product generated the data																										
Received	The date and time Apex Central received the data from the managed product																										
Endpoint	The name of the endpoint																										
Product	The name of the managed product or service																										
Managing Server Entity	The display name of the managed product server in Apex Central to which the endpoint reports																										
Product Version	The version of the managed product																										
Endpoint IP	The IP address of the endpoint																										
Risk Level	The risk level assigned by Attack Discovery																										
Pattern Version	The Attack Discovery pattern number for the detection type																										
Rule ID	The serial number of the detection rule																										
Rule Name	The rules which specify behaviors to be detected by Attack Discovery																										
Related Objects	The number of detections Click the count to view additional details.																										

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability	
		For more information, see Detailed Attack Discovery Detection Information on page B-11.
	Generated (Local Time)	The time in the agent's local timezone when Attack Discovery detected the threat The time is displayed with the UTC offset.
	Instance ID	The detection ID assigned to the event Entries having the same instance ID belong under the same event.
	Tactics	The MITRE ATT&CK™ tactic(s) detected For more information, see https://attack.mitre.org/tactics/enterprise/ .
	Techniques	The MITRE ATT&CK™ technique(s) detected For more information, see https://attack.mitre.org/techniques/enterprise/ .
<p><i>Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-10</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“Threat Encyclopedia</p> <p>Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. <u>The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.</u></p>		

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability				
	<p>Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:</p> <ul style="list-style-type: none"> • Malware and malicious mobile code currently active or "in the wild" • Correlated threat information pages to form a complete web attack story • Internet threat advisories about targeted attacks and security threats • Web attack and online trend information • Weekly malware reports" <p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 25-2 to 25-3 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>				
<p>cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;</p>	<p>Trend Micro Apex Central is configured to <i>cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type (e.g., firewall configuration, etc.) and a other occurrence mitigation type (e.g., intrusion detection, etc.), across the plurality of devices (e.g., managed products and endpoints, etc.) for occurrence mitigation by preventing advantage being taken of actual vulnerabilities (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types e.g., firewall configuration, intrusion detection, etc.) across the plurality of devices (e.g., managed products and endpoints, etc.);</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <table border="1" data-bbox="661 1287 1911 1404"> <tr> <th data-bbox="661 1287 1010 1330">Consideration</th><th data-bbox="1010 1287 1911 1330">Effect</th></tr> <tr> <td data-bbox="661 1330 1010 1404">Deployment planning</td><td data-bbox="1010 1330 1911 1404"><u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to</u></td></tr> </table>	Consideration	Effect	Deployment planning	<u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to</u>
Consideration	Effect				
Deployment planning	<u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to</u>				

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability	
		<p><u>products based on Deployment Plans</u>. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</p>
	<p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 10-13 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf</p>	
	<p>“Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system</p>	
	<p>...</p>	
	<p>Table 1. Product Status Information Data View</p>	
	Operating System	The operating system on the managed product server or Security Agent endpoint
	OS Version	The version of the operating system on the managed product server or Security Agent endpoint
	OS Service Pack	The service pack number of the operating system on the managed product server or Security Agent endpoint
	<p>Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center</p>	
	<p>“ ... 5. In the Certified Safe Software List section, configure the following:</p>	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability
	<ul style="list-style-type: none"> • Enable the local Certified Safe Software List: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. • Enable the global Certified Safe Software List (Internet access required): Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. <p>Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.</p> <p>6. In the Exception section, manage the Exception Template List that applies to this policy only. <u>The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.</u></p> <p>For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3).</p> <p>7. Click Save. https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)</p> <p>“Detailed Firewall Violation Information</p> <p>Provides <u>specific firewall configuration information on your network</u>, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations”</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability	
	Section	Settings
	Received	The date and time Apex Central received the data from the managed product
	Generated	The date and time the managed product generated the data
	Product Entity/Endpoint	Depending on the related source: <ul style="list-style-type: none"> • The display name of the managed product server in Apex Central • The name or IP address of the endpoint Product
	Product	The name of the managed product or service Example: Apex One, ScanMail for Microsoft Exchange
	Event Type	The type of event that triggered the detection Example: intrusion, policy violation
	Risk Level	The Trend Micro assessment of risk to your network Example: High security, low security, medium security
	Traffic/Connection	The direction of the transmission
	Protocol	The protocol the intrusion uses Example: HTTP, SMTP, FTP
	Source IP	The source IP address of the detected threat
	Endpoint Port	The port number of the endpoint under attack
	Endpoint IP	The IP address of the endpoint
	Target Application	The application the intrusion targeted

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability								
	Description	The detailed description of the incident by Trend Micro							
	Action	The action taken by the managed product Example: file cleaned, file quarantined, file passed							
	Detections	The total number of detections Example: A managed product detects 10 violation instances of the same type on one computer Detections = 10							
	Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)								
	<table><tr><th>Feature</th><th>Description</th></tr><tr><td>...</td><td>...</td></tr><tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by <u>automating the application of virtual patches before official patches become available</u>. Trend Micro provides protected endpoints with <i>recommended Intrusion Prevention</i> rules based on your network performance and security priorities.</td></tr><tr><td>...</td><td>...</td></tr></table>		Feature	Description	Vulnerability Protection Integration	Integration with Vulnerability Protection protects Apex One users by <u>automating the application of virtual patches before official patches become available</u> . Trend Micro provides protected endpoints with <i>recommended Intrusion Prevention</i> rules based on your network performance and security priorities.	...
Feature	Description								
...	...								
Vulnerability Protection Integration	Integration with Vulnerability Protection protects Apex One users by <u>automating the application of virtual patches before official patches become available</u> . Trend Micro provides protected endpoints with <i>recommended Intrusion Prevention</i> rules based on your network performance and security priorities.								
...	...								
https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx									
“Intrusion Prevention Rules									

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability								
	<p>The Intrusion Prevention Rules screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.</p> <ul style="list-style-type: none"> • To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule.” <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 14-33 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“The Threat Type column displays the following threat types.</p> <table border="1" data-bbox="661 1006 1911 1360"> <thead> <tr> <th data-bbox="661 1006 1008 1047">Threat Type</th><th data-bbox="1008 1006 1911 1047">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="661 1047 1008 1128">Ransomware</td><td data-bbox="1008 1047 1911 1128">Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr> <tr> <td data-bbox="661 1128 1008 1282"><u>Known Advanced Persistent Threat (APT)</u></td><td data-bbox="1008 1128 1911 1282"><u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u></td></tr> <tr> <td data-bbox="661 1282 1008 1360">Social engineering attack</td><td data-bbox="1008 1282 1911 1360">Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr> </tbody> </table>	Threat Type	Description	Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid	<u>Known Advanced Persistent Threat (APT)</u>	<u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u>	Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file
Threat Type	Description								
Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid								
<u>Known Advanced Persistent Threat (APT)</u>	<u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u>								
Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file								

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability	
	Vulnerability attack	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems
	Lateral movement	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
	Unknown threats	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer
	C&C callback	Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware
wherein the at least one configuration involves at least one operating system.	<p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 3-20 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>	
	<p>Trend Micro Apex Central is configured <i>wherein the at least one configuration</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>involves at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.).</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Vulnerability attack</p>	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 1 Elements	Applicability
	<p>Malware or hacker attacks that <u>exploits a security weakness typically found in programs and operating systems</u> (pg 3-10)”</p> <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 3-10 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“Procedure</p> <ol style="list-style-type: none"> 1. Go to Administration > Security Agent Download. 2. Select the operating system. <ul style="list-style-type: none"> • Windows 64-bit: Select to create a 64-bit MSI installation package for Apex One Security Agents • Windows 32-bit: Select to create a 32-bit MSI installation package for Apex One Security Agents • Mac OS: Select to create a ZIP installation package for Apex One (Mac) Security Agents” <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 9-3 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability																		
The non-transitory computer-readable media of Claim 1, wherein the at least one actual vulnerability is one of the actual vulnerabilities that are of the at least operating system that is installed on the plurality of devices, the occurrence is at least one of a plurality of occurrences, and the instructions include:	<p>Trend Micro Apex Central infringes claim 1 and includes <i>the non-transitory computer-readable media of Claim 1, wherein the at least one actual vulnerability is one of the actual vulnerabilities (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) that are of the at least operating system (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) that is installed on the plurality of devices (e.g., managed products and endpoints, etc.), the occurrence (e.g., the positively-identified attack based on one of the known threat types, etc.) is at least one of a plurality of occurrences, and the instructions include:</i></p> <p>Note: See, for example, the evidence below (emphasis added, if any):</p> <p>“Attack Discovery Detection Information</p> <p><u>Provides general information about threats detected by Attack Discovery</u></p> <table> <tr> <th>Data</th><th>Description</th></tr> <tr> <td>Generated</td><td>The date and time the managed product generated the data</td></tr> <tr> <td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr> <tr> <td>Endpoint</td><td>The name of the endpoint</td></tr> <tr> <td>Product</td><td>The name of the managed product or service</td></tr> <tr> <td>Managing Server Entity</td><td>The display name of the managed product server in Apex Central to which the endpoint reports</td></tr> <tr> <td>Product Version</td><td>The version of the managed product</td></tr> <tr> <td>Endpoint IP</td><td>The IP address of the endpoint</td></tr> <tr> <td>Risk Level</td><td>The risk level assigned by Attack Discovery</td></tr> </table>	Data	Description	Generated	The date and time the managed product generated the data	Received	The date and time Apex Central received the data from the managed product	Endpoint	The name of the endpoint	Product	The name of the managed product or service	Managing Server Entity	The display name of the managed product server in Apex Central to which the endpoint reports	Product Version	The version of the managed product	Endpoint IP	The IP address of the endpoint	Risk Level	The risk level assigned by Attack Discovery
Data	Description																		
Generated	The date and time the managed product generated the data																		
Received	The date and time Apex Central received the data from the managed product																		
Endpoint	The name of the endpoint																		
Product	The name of the managed product or service																		
Managing Server Entity	The display name of the managed product server in Apex Central to which the endpoint reports																		
Product Version	The version of the managed product																		
Endpoint IP	The IP address of the endpoint																		
Risk Level	The risk level assigned by Attack Discovery																		

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Pattern Version	The Attack Discovery pattern number for the detection type
	Rule ID	The serial number of the detection rule
	Rule Name	The rules which specify behaviors to be detected by Attack Discovery
	Related Objects	<p>The number of detections</p> <p>Click the count to view additional details.</p> <p>For more information, see Detailed Attack Discovery Detection Information on page B-11.</p>
	Generated (Local Time)	<p>The time in the agent's local timezone when Attack Discovery detected the threat</p> <p>The time is displayed with the UTC offset.</p>
	Instance ID	<p>The detection ID assigned to the event</p> <p>Entries having the same instance ID belong under the same event.</p>
	Tactics	<p>The MITRE ATT&CK™ tactic(s) detected</p> <p>For more information, see https://attack.mitre.org/tactics/enterprise/.</p>
	Techniques	<p>The MITRE ATT&CK™ technique(s) detected</p> <p>For more information, see https://attack.mitre.org/techniques/enterprise/.</p>
<p><i>Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-10</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>		

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>“Vulnerability attack</p> <p>Malware or hacker attacks that <u>exploits a security weakness typically found in programs and operating systems</u> (pg 3-10)”</p> <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 3-10 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“Procedure</p> <ol style="list-style-type: none"> 1. Go to Administration > Security Agent Download. 2. Select the operating system. <ul style="list-style-type: none"> • Windows 64-bit: Select to create a 64-bit MSI installation package for Apex One Security Agents • Windows 32-bit: Select to create a 32-bit MSI installation package for Apex One Security Agents • Mac OS: Select to create a ZIP installation package for Apex One (Mac) Security Agents” <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 9-3 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“About Apex Central</p> <p>Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. <u>Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints</u>. The Apex Central web-based management console <u>provides a single monitoring point for antivirus and content security products and services throughout the network</u>. Apex Central enables system administrators to monitor and report on</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy components, such as antivirus pattern files, scan engines, and antispam rules, throughout the network to ensure up-to-date protection. Apex Central allows both manual and pre-scheduled updates, and allows the configuration and administration of products as groups or as individuals for added flexibility.”</p> <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 1-2 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>
<p>first instructions that, when executed by at least one first processor of the one or more processors of at least one server in communication with the at least one second storage, cause the at least one first processor to:</p> <p>generate the first vulnerability information utilizing the second vulnerability information, and</p>	<p>Trend Micro Apex Central infringes claim 1 and includes <i>first instructions that, when executed by at least one first processor of the one or more processors of at least one server</i> (e.g., one or more servers that includes, accesses, and/or serves Trend Micro Apex Central, etc.) <i>in communication with the at least one second storage</i> (e.g., a Common Vulnerabilities and Exposures (CVE) database, etc.), <i>cause the at least one first processor to: generate the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>utilizing the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof), <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Understanding the Apex Central Database</p> <p><u>Apex Central uses the Microsoft SQL Server database (db ApexCentral.mdf) to store data included in logs, Communicator schedule, memory on the at least one device, user account, network environment, and notification settings.</u></p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability										
	<p>The Apex Central server establishes the database connection using a System DSN ODBC connection. The Apex Central installation generates this connection as well as the ID and password used to access db_ApexCentral.mdf. The default ID is sa. Apex Central encrypts the password.</p> <p>To maximize the SQL server security, configure any SQL account used to manage db_ApexCentral with the following minimum permissions:</p> <ul style="list-style-type: none"> • dbcreator for the server role • db_owner role for db_ApexCentral <p>Logs from managed products contribute to database expansion. Managed products send various log types to Apex Central.”</p> <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 23-2 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“Attack Discovery Detection Information</p> <p><u>Provides general information about threats detected by Attack Discovery</u></p> <table> <tr> <th>Data</th><th>Description</th></tr> <tr> <td>Generated</td><td>The date and time the managed product generated the data</td></tr> <tr> <td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr> <tr> <td>Endpoint</td><td>The name of the endpoint</td></tr> <tr> <td>Product</td><td>The name of the managed product or service</td></tr> </table>	Data	Description	Generated	The date and time the managed product generated the data	Received	The date and time Apex Central received the data from the managed product	Endpoint	The name of the endpoint	Product	The name of the managed product or service
Data	Description										
Generated	The date and time the managed product generated the data										
Received	The date and time Apex Central received the data from the managed product										
Endpoint	The name of the endpoint										
Product	The name of the managed product or service										

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Managing Server Entity	The display name of the managed product server in Apex Central to which the endpoint reports
	Product Version	The version of the managed product
	Endpoint IP	The IP address of the endpoint
	Risk Level	The risk level assigned by Attack Discovery
	Pattern Version	The Attack Discovery pattern number for the detection type
	Rule ID	The serial number of the detection rule
	Rule Name	The rules which specify behaviors to be detected by Attack Discovery
	Related Objects	<p>The number of detections</p> <p>Click the count to view additional details.</p> <p>For more information, see Detailed Attack Discovery Detection Information on page B-11.</p>
	Generated (Local Time)	<p>The time in the agent's local timezone when Attack Discovery detected the threat</p> <p>The time is displayed with the UTC offset.</p>
	Instance ID	<p>The detection ID assigned to the event</p> <p>Entries having the same instance ID belong under the same event.</p>
	Tactics	<p>The MITRE ATT&CK™ tactic(s) detected</p> <p>For more information, see https://attack.mitre.org/tactics/enterprise/.</p>
	Techniques	The MITRE ATT&CK™ technique(s) detected

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<div data-bbox="661 336 1911 451"> <div></div> <div>For more information, see https://attack.mitre.org/techniques/enterprise/.</div> </div> <p data-bbox="661 456 1745 529"><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page B-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p data-bbox="661 573 945 605">“Threat Encyclopedia</p> <p data-bbox="661 654 1911 846">Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. <u>The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.</u></p> <p data-bbox="661 894 1841 959">Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:</p> <ul data-bbox="661 976 1663 1162" style="list-style-type: none"> • Malware and malicious mobile code currently active or "in the wild" • Correlated threat information pages to form a complete web attack story • Internet threat advisories about targeted attacks and security threats • Web attack and online trend information • Weekly malware reports” <p data-bbox="661 1170 1745 1243"><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 25-2 to 25-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>
communicate, from the at least one server and to the at least one of the plurality of devices	Trend Micro Apex Central infringes claim 1 and is configured to <i>communicate, from the at least one server</i> (e.g., one or more servers that includes, accesses, and/or serves Trend Micro Apex Central, etc.) <i>and to the at least one of the plurality of devices</i> (e.g., one of the managed products

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability								
over at least one network, the first vulnerability information;	<p>and endpoints, etc.) <i>over at least one network, the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“About the Web Console</p> <p>The Apex Central web console provides centralized management, monitoring, and security visibility for all endpoints and users protected by Trend Micro products registered to the Apex Central server. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. <u>The web console lets you administer the Apex Central network from any machine using a compatible web browser.</u></p> <p>Apex Central supports the following web browsers:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer™ 11 • Microsoft Edge™ • Google Chrome™ <p>Web Console Requirements</p> <table> <tr> <th>Resource</th><th>Requirement</th></tr> <tr> <td>Processor</td><td>300 MHz Intel™ Pentium™ processor or equivalent</td></tr> <tr> <td>RAM</td><td>128 MB minimum</td></tr> <tr> <td>Available disk space</td><td>30 MB minimum</td></tr> </table>	Resource	Requirement	Processor	300 MHz Intel™ Pentium™ processor or equivalent	RAM	128 MB minimum	Available disk space	30 MB minimum
Resource	Requirement								
Processor	300 MHz Intel™ Pentium™ processor or equivalent								
RAM	128 MB minimum								
Available disk space	30 MB minimum								

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Browser	<p>Microsoft Internet Explorer™ 11, Microsoft Edge™, or Google Chrome™</p> <p>Important: When using Internet Explorer to access the Apex Central web console, turn off Compatibility View.</p>
<p>second instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the second instructions are executed by at least one second processor of the one or more processors of the at least one of the plurality of devices, cause the at least one second processor to:</p> <p>receive, from the at least one server and at the at least one of the plurality of devices over the at least one network, the first vulnerability information,</p>	<p><i>Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 2-2 to 2-3</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf</p> <p>Trend Micro Apex Central infringes claim 1 and includes <i>second instructions that are configured to be stored on the at least one first data storage</i> (e.g., memory on the at least one device, etc.) <i>which is part of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.) <i>and that, when the second instructions are executed by at least one second processor of the one or more processors of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.), <i>cause the at least one second processor to: receive, from the at least one server</i> (e.g., one or more servers that includes, accesses, and/or serves Trend Micro Apex Central, etc.) <i>and at the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.) <i>over the at least one network, the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof),</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Understanding the Apex Central Database</p>	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p><u>Apex Central uses the Microsoft SQL Server database (db_ApexCentral.mdf) to store data included in logs, Communicator schedule, memory on the at least one device, user account, network environment, and notification settings.</u></p> <p>The Apex Central server establishes the database connection using a System DSN ODBC connection. The Apex Central installation generates this connection as well as the ID and password used to access db_ApexCentral.mdf. The default ID is sa. Apex Central encrypts the password.</p> <p>To maximize the SQL server security, configure any SQL account used to manage db_ApexCentral with the following minimum permissions:</p> <ul style="list-style-type: none"> • dbcreator for the server role • db_owner role for db_ApexCentral <p>Logs from managed products contribute to database expansion. Managed products send various log types to Apex Central.”</p> <p><i>Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 23-2</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>Note: As set forth below, Trend Micro Apex Central includes software that generates (and communicates to the managed products and endpoints) at least a portion of the first vulnerability information (e.g., signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software) utilizing the second vulnerability information (e.g., ALL signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software available at the Trend Micro ActiveUpdate server and/or other update servers). As set forth below, once configured, the Trend Micro ActiveUpdate</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability								
	<p>server and/or other servers automatically determine which of the updates to generate and communicate.</p> <table border="1"> <tr> <th>Consideration</th><th>Effect</th></tr> <tr> <td>Deployment planning</td><td>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to <u>products based on Deployment Plans</u>. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr> </table> <p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 10-13 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system</p> <p>...</p> <p>Table 1. Product Status Information Data View</p> <table border="1"> <tr> <td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr> <tr> <td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr> </table>	Consideration	Effect	Deployment planning	Apex Central deploys update components (for example, virus pattern files , scan engines , anti-spam rules, program updates) to <u>products based on Deployment Plans</u> . These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.	Operating System	The operating system on the managed product server or Security Agent endpoint	OS Version	The version of the operating system on the managed product server or Security Agent endpoint
Consideration	Effect								
Deployment planning	Apex Central deploys update components (for example, virus pattern files , scan engines , anti-spam rules, program updates) to <u>products based on Deployment Plans</u> . These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.								
Operating System	The operating system on the managed product server or Security Agent endpoint								
OS Version	The version of the operating system on the managed product server or Security Agent endpoint								

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	OS Service Pack	The service pack number of the operating system on the managed product server or Security Agent endpoint
	Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center	
	Feature	Description

	Vulnerability Protection Integration	Integration with Vulnerability Protection protects Apex One users by <u>automating the application of virtual patches before official patches become available</u> . Trend Micro provides protected endpoints with <i>recommended Intrusion Prevention</i> rules based on your network performance and security priorities.

	https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx	
	<p>“Intrusion Prevention Rules</p> <p>The Intrusion Prevention Rules screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.</p> <ul style="list-style-type: none"> To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. 	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<ul style="list-style-type: none"> To sort the list of Intrusion Prevention Rules by column data, click a column heading. To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule.” <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 14-33 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf</p> <p>“ ...</p> <p>5. In the Certified Safe Software List section, configure the following:</p> <ul style="list-style-type: none"> Enable the local Certified Safe Software List: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. Enable the global Certified Safe Software List (Internet access required): Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. <p>Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.</p> <p>6. In the Exception section, manage the Exception Template List that applies to this policy only. <u><i>The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.</i></u></p> <p>For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3).</p> <p>7. Click Save.”</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)
store the first vulnerability information on the at least one first data storage, and	<p>Trend Micro Apex Central infringes claim 1 and is configured to <i>store the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>on the at least one first data storage</i> (e.g., memory on the at least one device, etc.), <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“Understanding the Apex Central Database</p> <p>Apex Central uses the Microsoft SQL Server database (db_ApexCentral.mdf) to store data included in logs, Communicator schedule, memory on the at least one device, user account, network environment, and notification settings.</p> <p>The Apex Central server establishes the database connection using a System DSN ODBC connection. The Apex Central installation generates this connection as well as the ID and password used to access db_ApexCentral.mdf. The default ID is sa. Apex Central encrypts the password.</p> <p>To maximize the SQL server security, configure any SQL account used to manage db_ApexCentral with the following minimum permissions:</p> <ul style="list-style-type: none"> • dbcreator for the server role • db_owner role for db_ApexCentral

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p><u>Logs from managed products contribute to database expansion. Managed products send various log types to Apex Central.</u></p> <p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 23-2 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>
<p>receive the first vulnerability information from the at least one first data storage, the first vulnerability information being relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and excluding at least a portion of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices;</p>	<p>Trend Micro Apex Central infringes claim 1 and is configured to <i>receive the first vulnerability information</i> (e.g., the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>from the at least one first data storage</i> (e.g., memory on the at least one device, etc.), <i>the first vulnerability information being relevant to the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.), <i>and excluding at least a portion of the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is not relevant to the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: As set forth below, Trend Micro Apex Central includes software that generates (and communicates to the managed products and endpoints) at least a portion of the first</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability				
	<p>vulnerability information (e.g., signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software) utilizing the second vulnerability information (e.g., ALL signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software available at the Trend Micro ActiveUpdate server and/or other update servers). As set forth below, once configured, the Trend Micro ActiveUpdate server and/or other servers automatically determine which of the updates to generate and communicate.</p> <table border="1" data-bbox="661 646 1911 922"> <tr> <th data-bbox="661 646 1012 688">Consideration</th><th data-bbox="1012 646 1911 688">Effect</th></tr> <tr> <td data-bbox="661 688 1012 922">Deployment planning</td><td data-bbox="1012 688 1911 922"><u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans.</u> These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr> </table> <p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 10-13 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system</p> <p>...</p> <p>Table 1. Product Status Information Data View</p>	Consideration	Effect	Deployment planning	<u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans.</u> These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.
Consideration	Effect				
Deployment planning	<u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans.</u> These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.				

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Operating System	The operating system on the managed product server or Security Agent endpoint
	OS Version	The version of the operating system on the managed product server or Security Agent endpoint
	OS Service Pack	The service pack number of the operating system on the managed product server or Security Agent endpoint
	Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center	
	Feature	Description

	Vulnerability Protection Integration	Integration with Vulnerability Protection protects Apex One users by <u>automating the application of virtual patches before official patches become available</u> . Trend Micro provides protected endpoints with <i>recommended Intrusion Prevention</i> rules based on your network performance and security priorities.

	https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx	
	<p>“Intrusion Prevention Rules</p> <p>The Intrusion Prevention Rules screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include</p>	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.</p> <ul style="list-style-type: none"> • To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule.” <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 14-33 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“ ...</p> <p>5. In the Certified Safe Software List section, configure the following:</p> <ul style="list-style-type: none"> • Enable the local Certified Safe Software List: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. • Enable the global Certified Safe Software List (Internet access required): Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. <p>Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.</p> <p>6. In the Exception section, manage the Exception Template List that applies to this policy only. <u>The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.</u></p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3).</p> <p>7. Click Save."</p> <p>https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)</p>
<p>third instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the third instructions are executed by the at least one second processor, cause the at least one second processor to:</p> <p>identify a first portion of the first vulnerability information that includes data inspection-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other data</p>	<p>Trend Micro Apex Central infringes claim 1 and includes <i>third instructions that are configured to be stored on the at least one first data storage</i> (e.g., memory on the at least one device, etc.) <i>which is part of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.) <i>and that, when the third instructions are executed by the at least one second processor, cause the at least one second processor to: identify a first portion of the first vulnerability information</i> (e.g., a first portion of the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>that includes data inspection-related information</i> (e.g., antivirus pattern information or the data loss prevention information, etc.) <i>that is relevant to at least one of the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.), <i>and that excludes other data inspection-related information of the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is not relevant to the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof,</p>



PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
inspection-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices,	etc.) of the at least one of the plurality of devices (e.g., one of the managed products and endpoints, etc.),	
	Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):	
	Consideration	Effect
	Deployment planning	<u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans.</u> These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.
	Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)	
	“Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system	
	...	
	Table 1. Product Status Information Data View	
	Operating System	The operating system on the managed product server or Security Agent endpoint

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability				
	OS Version	The version of the operating system on the managed product server or Security Agent endpoint			
	OS Service Pack	The service pack number of the operating system on the managed product server or Security Agent endpoint			
	Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center				
	<p>“Compliance Indicators</p> <div><div><div>75% Antivirus pattern compliance -</div><div>Endpoints with outdated patterns: 1</div></div><div><div>0% Data Loss Prevention compliance -</div><div>Endpoints with unacceptable threat detections: 4</div></div></div> <p>This section of the Operation Center tab <u>provides information about the antivirus pattern information or the data loss prevention information</u> level of your network.</p> <p>As your network compliance level changes, the color of the compliance indicator icon changes to reflect the thresholds configured on the Active Directory and Compliance Settings screen.</p> <p>The default view displays information for the Antivirus pattern compliance indicator.”</p> <p><i>Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 3-7</i></p> <p>https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf</p> <table><tr><th>Update Method</th><th>Description</th></tr><tr><td><u>Antivirus pattern compliance</u></td><td>Displays the following information:</td></tr></table>		Update Method	Description	<u>Antivirus pattern compliance</u>
Update Method	Description				
<u>Antivirus pattern compliance</u>	Displays the following information:				

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<div data-bbox="1024 336 1927 646"> <ul style="list-style-type: none"> • The percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions • The total number of endpoints with outdated antivirus patterns on your network <p>Click the count for Endpoints with outdated patterns to view detailed information about the affected endpoints in the User/Endpoint Directory.</p> </div> <p><i>Trend Micro Apex Central Widget and Policy Management Guide, Version: 2019, Page 1-7 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_wpg.pdf)</i></p>
<p>identify a first occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and</p> <p>cause a determination whether the at least one of the actual vulnerabilities relevant to the data inspection-related information is susceptible to being taken advantage of by the first occurrence identified in connection with the at least one of the plurality of devices, utilizing the data inspection-related information;</p>	<p>Trend Micro Apex Central infringes claim 1 and is configured to <i>identify a first occurrence</i> (e.g., a first discrete event that triggers at least one of the signature/policy updates for the anti-virus/data loss prevention software, etc.) <i>of the plurality of occurrences in connection with the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.), <i>and cause a determination whether the at least one of the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>relevant to the data inspection-related information</i> (e.g., antivirus pattern information or the data loss prevention information, etc.) <i>is susceptible to being taken advantage of by the first occurrence</i> (e.g., a first discrete event that triggers at least one of the signature/policy updates for the anti-virus/data loss prevention software, etc.) <i>identified in connection with the at least one of the plurality of devices</i> e.g., one of the managed products and endpoints, etc.), <i>utilizing the data inspection-related information</i> (e.g., antivirus pattern information or the data loss prevention information, etc.);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability				
	<p>Note: Antivirus pattern compliance includes signatures/policies that are triggered by some events (e.g., the first occurrence, etc.), so that malicious events (relevant to the device's operating system) trigger a response.</p> <table border="1"> <thead> <tr> <th data-bbox="661 532 1012 574">Indicator</th><th data-bbox="1012 532 1921 574">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="661 574 1012 1385"> <u>Antivirus pattern compliance</u> </td><td data-bbox="1012 574 1921 1385"> <p>Displays the percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions</p> <p>You can also view the following details:</p> <ul style="list-style-type: none"> • Managed agents: The number of endpoints that have Security Agents installed <ul style="list-style-type: none"> ○ With compliant virus patterns: The number of managed agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions ○ With outdated virus patterns: The number of managed agents not using acceptable Virus Pattern and Smart Scan Agent Pattern versions ○ Offline for 7 days: The number of managed agents that have not communicated with the managed product server in 7 or more days ○ Exceptions: The number of users or endpoints excluded from the compliance calculations • Unmanaged endpoints: The number of endpoints that do not have Security Agents installed </td></tr> </tbody> </table>	Indicator	Description	<u>Antivirus pattern compliance</u>	<p>Displays the percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions</p> <p>You can also view the following details:</p> <ul style="list-style-type: none"> • Managed agents: The number of endpoints that have Security Agents installed <ul style="list-style-type: none"> ○ With compliant virus patterns: The number of managed agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions ○ With outdated virus patterns: The number of managed agents not using acceptable Virus Pattern and Smart Scan Agent Pattern versions ○ Offline for 7 days: The number of managed agents that have not communicated with the managed product server in 7 or more days ○ Exceptions: The number of users or endpoints excluded from the compliance calculations • Unmanaged endpoints: The number of endpoints that do not have Security Agents installed
Indicator	Description				
<u>Antivirus pattern compliance</u>	<p>Displays the percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions</p> <p>You can also view the following details:</p> <ul style="list-style-type: none"> • Managed agents: The number of endpoints that have Security Agents installed <ul style="list-style-type: none"> ○ With compliant virus patterns: The number of managed agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions ○ With outdated virus patterns: The number of managed agents not using acceptable Virus Pattern and Smart Scan Agent Pattern versions ○ Offline for 7 days: The number of managed agents that have not communicated with the managed product server in 7 or more days ○ Exceptions: The number of users or endpoints excluded from the compliance calculations • Unmanaged endpoints: The number of endpoints that do not have Security Agents installed 				

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<div data-bbox="661 334 1911 412"> Expand the categories and click a count to view additional details about the affected endpoints. </div> <div data-bbox="661 417 1911 495"> <i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 3-10 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf </div>
<p>fourth instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the fourth instructions are executed by the at least one second processor, cause the at least one second processor to:</p> <p>identify a second portion of the first vulnerability information that includes traffic inspection-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other traffic inspection-related information of the second</p>	<p>Trend Micro Apex Central infringes claim 1 and includes <i>fourth instructions that are configured to be stored on the at least one first data storage</i> (e.g., memory on the at least one device, etc.) <i>which is part of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.) <i>and that, when the fourth instructions are executed by the at least one second processor, cause the at least one second processor to: identify a second portion of the first vulnerability information</i> (e.g., a second portion of the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>that includes traffic inspection-related information</i> (e.g., intrusion detection rules, etc.) <i>that is relevant to at least one of the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.), <i>and that excludes other traffic inspection-related information of the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is not relevant to the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.),</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices,	Consideration	Effect
	Deployment planning	Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to <u>products based on Deployment Plans</u> . These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.
	Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)	
	"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system	
	...	
	Table 1. Product Status Information Data View	
	Operating System	The operating system on the managed product server or Security Agent endpoint
	OS Version	The version of the operating system on the managed product server or Security Agent endpoint
	OS Service Pack	The service pack number of the operating system on the managed product server or Security Agent endpoint

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability								
	<p data-bbox="661 337 1661 370">Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center</p> <table border="1" data-bbox="661 410 1906 727"> <thead> <tr> <th data-bbox="667 415 1010 451">Feature</th><th data-bbox="1010 415 1900 451">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="667 456 1010 492">...</td><td data-bbox="1010 456 1900 492">...</td></tr> <tr> <td data-bbox="667 496 1010 686">Vulnerability Protection Integration</td><td data-bbox="1010 496 1900 686">Integration with Vulnerability Protection protects Apex One users by <u>automating the application of virtual patches before official patches become available</u>. Trend Micro provides protected endpoints with <i>recommended Intrusion Prevention</i> rules based on your network performance and security priorities.</td></tr> <tr> <td data-bbox="667 691 1010 727">...</td><td data-bbox="1010 691 1900 727">...</td></tr> </tbody> </table> <p data-bbox="661 735 1782 805">https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx</p> <p data-bbox="661 854 1026 881">“Intrusion Prevention Rules</p> <p data-bbox="661 935 1923 1162">The Intrusion Prevention Rules screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.</p> <ul data-bbox="667 1211 1917 1399" style="list-style-type: none"> • To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule.” 	Feature	Description	Vulnerability Protection Integration	Integration with Vulnerability Protection protects Apex One users by <u>automating the application of virtual patches before official patches become available</u> . Trend Micro provides protected endpoints with <i>recommended Intrusion Prevention</i> rules based on your network performance and security priorities.
Feature	Description								
...	...								
Vulnerability Protection Integration	Integration with Vulnerability Protection protects Apex One users by <u>automating the application of virtual patches before official patches become available</u> . Trend Micro provides protected endpoints with <i>recommended Intrusion Prevention</i> rules based on your network performance and security priorities.								
...	...								

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability						
	<p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 14-33 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“ ...</p> <p>5. In the Certified Safe Software List section, configure the following:</p> <ul style="list-style-type: none"> • Enable the local Certified Safe Software List: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. • Enable the global Certified Safe Software List (Internet access required): Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. <p>Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.” https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)</p> <p>“The Threat Type column displays the following threat types.</p> <table border="1" data-bbox="661 1084 1911 1360"> <thead> <tr> <th data-bbox="661 1084 1012 1127">Threat Type</th><th data-bbox="1012 1084 1911 1127">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="661 1127 1012 1208">Ransomware</td><td data-bbox="1012 1127 1911 1208">Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr> <tr> <td data-bbox="661 1208 1012 1360"><u>Known Advanced Persistent Threat (APT)</u></td><td data-bbox="1012 1208 1911 1360"><u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u></td></tr> </tbody> </table>	Threat Type	Description	Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid	<u>Known Advanced Persistent Threat (APT)</u>	<u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u>
Threat Type	Description						
Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid						
<u>Known Advanced Persistent Threat (APT)</u>	<u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u>						

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file
	Vulnerability attack	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems
	Lateral movement	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
	Unknown threats	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer
	C&C callback	Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware
	Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)	
identify a second occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and cause a determination whether the at least one of the actual vulnerabilities relevant to the traffic inspection-related	Trend Micro Apex Central infringes claim 1 and is configured to <i>identify a second occurrence</i> (e.g., a second discrete event that triggers at least one of the signature/policy updates for the intrusion prevention rules, etc.) <i>of the plurality of occurrences in connection with the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.), <i>and cause a determination whether the at least one of the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>relevant to the traffic inspection-related information</i> (e.g., intrusion detection rules, etc.) <i>is susceptible to being taken advantage of by the second occurrence</i> (e.g., a second discrete event that triggers at least one of the signature/policy updates for the intrusion prevention rules, etc.)	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
<p>information is susceptible to being taken advantage of by the second occurrence identified in connection with the at least one of the plurality of devices, utilizing the traffic inspection-related information;</p>	<p><i>identified in connection with the at least one of the plurality of devices (e.g., one of the managed products and endpoints, etc.), utilizing the traffic inspection-related information (e.g., intrusion detection rules, etc.);</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: The intrusion prevention rules include signatures/policies that are triggered by some events (e.g., the third event, etc.), and that are not triggered by other events (e.g., the fourth event, etc.), so that only malicious events (relevant to the device's operating system) trigger a response.</p> <p>"Intrusion Prevention Rules</p> <p>The Intrusion Prevention Rules screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). <u>Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.</u></p> <ul style="list-style-type: none"> • To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule."

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 14-33 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>
<p>fifth instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the fifth instructions are executed by the at least one second processor, cause the at least one second processor to:</p> <p>identify a third portion of the first vulnerability information that includes firewall-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other firewall-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one</p>	<p>Trend Micro Apex Central infringes claim 1 and includes <i>fifth instructions that are configured to be stored on the at least one first data storage</i> (e.g., memory on the at least one device, etc.) <i>which is part of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.) <i>and that, when the fifth instructions are executed by the at least one second processor, cause the at least one second processor to: identify a third portion of the first vulnerability information</i> (e.g., a third portion of the smaller “sub-set” of actual vulnerabilities relevant to a particular operating system/application/version thereof) <i>that includes firewall-related information</i> (e.g., firewall configuration information, etc.) <i>that is relevant to at least one of the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.), <i>and that excludes other firewall-related information of the second vulnerability information</i> (e.g., the larger “super-set” list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) <i>that is not relevant to the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>of the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>of the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.),</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
operating system of the at least one of the plurality of devices,	Consideration	Effect
	Deployment planning	Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.
	Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)	
	“Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system	
	...	
Table 1. Product Status Information Data View		
	Operating System	The operating system on the managed product server or Security Agent endpoint
	OS Version	The version of the operating system on the managed product server or Security Agent endpoint
	OS Service Pack	The service pack number of the operating system on the managed product server or Security Agent endpoint
Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center		

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>“ ...</p> <p>5. In the Certified Safe Software List section, configure the following:</p> <ul style="list-style-type: none"> • Enable the local Certified Safe Software List: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. • Enable the global Certified Safe Software List (Internet access required): Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. <p>Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.</p> <p>6. In the Exception section, manage the Exception Template List that applies to this policy only. <u>The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.</u></p> <p>For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3).</p> <p>7. Click Save.”</p> <p>https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)</p> <p>“Detailed Firewall Violation Information</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Provides <u>specific firewall configuration information on your network</u> , such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations”	
	Section	Settings
	Received	The date and time Apex Central received the data from the managed product
	Generated	The date and time the managed product generated the data
	Product Entity/Endpoint	Depending on the related source: <ul style="list-style-type: none"> • The display name of the managed product server in Apex Central • The name or IP address of the endpoint Product
	Product	The name of the managed product or service Example: Apex One, ScanMail for Microsoft Exchange
	Event Type	The type of event that triggered the detection Example: intrusion, policy violation
	Risk Level	The Trend Micro assessment of risk to your network Example: High security, low security, medium security
	Traffic/Connection	The direction of the transmission
	Protocol	The protocol the intrusion uses Example: HTTP, SMTP, FTP
	Source IP	The source IP address of the detected threat

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Endpoint Port	The port number of the endpoint under attack
	Endpoint IP	The IP address of the endpoint
	Target Application	The application the intrusion targeted
	Description	The detailed description of the incident by Trend Micro
	Action	The action taken by the managed product Example: file cleaned, file quarantined, file passed
	Detections	The total number of detections Example: A managed product detects 10 violation instances of the same type on one computer Detections = 10
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)		
<p>identify a third occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and</p> <p>cause a determination whether the at least one of the actual vulnerabilities relevant to the firewall-related information is susceptible to being taken advantage of by the third</p>	<p>Trend Micro Apex Central infringes claim 1 and is configured to <i>identify a third occurrence</i> (e.g., a third discrete event that triggers at least one of the signature/policy updates for the firewall violation software, etc.) <i>of the plurality of occurrences in connection with the at least one of the plurality of devices</i> (e.g., one of the managed products and endpoints, etc.), <i>and cause a determination whether the at least one of the actual vulnerabilities</i> (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) <i>relevant to the firewall-related information</i> (e.g., firewall configuration information, etc.) <i>is susceptible to being taken advantage of by the third occurrence</i> (e.g., a third discrete event that triggers at least one of the signature/policy updates for the firewall violation software, etc.) <i>identified in connection with the at least one of the plurality of devices</i> (e.g., one of the managed</p>	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
<p>occurrence identified in connection with the at least one of the plurality of devices, utilizing the firewall-related information; and</p>	<p>products and endpoints, etc.), <i>utilizing the firewall-related information</i> (e.g., firewall configuration information, etc.); <i>and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“ ...</p> <p>5. In the Certified Safe Software List section, configure the following:</p> <ul style="list-style-type: none"> • Enable the local Certified Safe Software List: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. • Enable the global Certified Safe Software List (Internet access required): Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. <p>Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.</p> <p>6. In the Exception section, manage the Exception Template List that applies to this policy only. <u>The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.</u></p> <p>For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3).</p> <p>7. Click Save.”</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability														
	<p>https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)</p> <p>“Detailed Firewall Violation Information</p> <p>Provides <u>specific firewall configuration information on your network</u>, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations”</p> <table> <tr> <th>Section</th><th>Settings</th></tr> <tr> <td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr> <tr> <td>Generated</td><td>The date and time the managed product generated the data</td></tr> <tr> <td>Product Entity/Endpoint</td><td>Depending on the related source: <ul style="list-style-type: none"> • The display name of the managed product server in Apex Central • The name or IP address of the endpoint Product </td></tr> <tr> <td>Product</td><td>The name of the managed product or service Example: Apex One, ScanMail for Microsoft Exchange</td></tr> <tr> <td>Event Type</td><td>The type of event that triggered the detection Example: intrusion, policy violation</td></tr> <tr> <td>Risk Level</td><td>The Trend Micro assessment of risk to your network Example: High security, low security, medium security</td></tr> </table>	Section	Settings	Received	The date and time Apex Central received the data from the managed product	Generated	The date and time the managed product generated the data	Product Entity/Endpoint	Depending on the related source: <ul style="list-style-type: none"> • The display name of the managed product server in Apex Central • The name or IP address of the endpoint Product 	Product	The name of the managed product or service Example: Apex One, ScanMail for Microsoft Exchange	Event Type	The type of event that triggered the detection Example: intrusion, policy violation	Risk Level	The Trend Micro assessment of risk to your network Example: High security, low security, medium security
Section	Settings														
Received	The date and time Apex Central received the data from the managed product														
Generated	The date and time the managed product generated the data														
Product Entity/Endpoint	Depending on the related source: <ul style="list-style-type: none"> • The display name of the managed product server in Apex Central • The name or IP address of the endpoint Product 														
Product	The name of the managed product or service Example: Apex One, ScanMail for Microsoft Exchange														
Event Type	The type of event that triggered the detection Example: intrusion, policy violation														
Risk Level	The Trend Micro assessment of risk to your network Example: High security, low security, medium security														

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Traffic/Connection	The direction of the transmission
	Protocol	The protocol the intrusion uses Example: HTTP, SMTP, FTP
	Source IP	The source IP address of the detected threat
	Endpoint Port	The port number of the endpoint under attack
	Endpoint IP	The IP address of the endpoint
	Target Application	The application the intrusion targeted
	Description	The detailed description of the incident by Trend Micro
	Action	The action taken by the managed product Example: file cleaned, file quarantined, file passed
	Detections	The total number of detections Example: A managed product detects 10 violation instances of the same type on one computer Detections = 10
	Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)	
sixth instructions that, when executed by at least one third processor of an administrator computer, cause the at least one third processor to:	Trend Micro Apex Central infringes claim 1 and includes <i>sixth instructions that, when executed by at least one third processor of an administrator computer</i> (e.g., any machine with a web console that lets you administer the Apex Central network, etc.), <i>cause the at least one third processor to: in response to administrator action</i> (e.g., user input, etc.), <i>cause setting, before the first occurrence</i> (e.g., a first discrete event that triggers at least one of the signature/policy updates for the anti-virus/data loss prevention software, etc.), <i>of a first policy</i> (e.g., a security policy	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability				
<p>in response to administrator action, cause setting, before the first occurrence, of a first policy for the third instructions that is applied to a group including each of the plurality of devices that has the at least one operating system installed thereon,</p>	<p>designed for use in enforcing antivirus pattern compliance or data loss prevention compliance, etc.) <i>for the third instructions that is applied to a group including each of the plurality of devices (e.g., managed products and endpoints, etc.) that has the at least one operating system (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) installed thereon,</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>“About the Web Console</p> <p>The Apex Central web console provides centralized management, monitoring, and security visibility for all endpoints and users protected by Trend Micro products registered to the Apex Central server. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. <u>The web console lets you administer the Apex Central network from any machine using a compatible web browser.</u></p> <p>Apex Central supports the following web browsers:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer™ 11 • Microsoft Edge™ • Google Chrome™ <p>Web Console Requirements</p> <table border="1" data-bbox="661 1287 1911 1365"> <thead> <tr> <th data-bbox="661 1287 1010 1330">Resource</th><th data-bbox="1010 1287 1911 1330">Requirement</th></tr> </thead> <tbody> <tr> <td data-bbox="661 1330 1010 1365">Processor</td><td data-bbox="1010 1330 1911 1365">300 MHz Intel™ Pentium™ processor or equivalent</td></tr> </tbody> </table>	Resource	Requirement	Processor	300 MHz Intel™ Pentium™ processor or equivalent
Resource	Requirement				
Processor	300 MHz Intel™ Pentium™ processor or equivalent				

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	RAM	128 MB minimum
	Available disk space	30 MB minimum
	Browser	Microsoft Internet Explorer™ 11, Microsoft Edge™, or Google Chrome™ Important: When using Internet Explorer to access the Apex Central web console, turn off Compatibility View.
	<p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 2-2 to 2-3 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf</p> <p>Note: As set forth below, a security policy is capable of being set for use in enforcing antivirus pattern compliance or data loss prevention compliance.</p> <p>“Each managed product provides <i>different policy settings</i> that you can <i>configure</i> and deploy to policy targets.” https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/policies/policy-management_001/policy-management_002/creating-a-new-polic.aspx (emphasis added)</p> <p>“Configuring the Antivirus Pattern Compliance Indicators</p> <p>You can configure settings and exceptions for the Antivirus Pattern Compliance indicators to display the percentage of managed Security Agents using acceptable antivirus pattern (Virus Pattern and Smart Scan Agent Pattern) versions on the Operation Center tab.</p> <ol style="list-style-type: none"> 1. Go to Administration > Settings > Active Directory and Compliance Settings. 2. Click the Compliance Indicator tab. 	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability						
	<p data-bbox="667 337 1184 370">3. Click Antivirus pattern compliance.</p> <p data-bbox="667 418 1503 451">The following table describes the available configuration options.</p> <table data-bbox="667 492 1908 695"> <tr> <th data-bbox="667 492 1010 532">Column</th><th data-bbox="1010 492 1908 532">Description</th></tr> <tr> <td data-bbox="667 532 1010 613">Acceptable pattern versions</td><td data-bbox="1010 532 1908 613">Specify the pattern versions for endpoints to be considered compliant.</td></tr> <tr> <td data-bbox="667 613 1010 695">Alert indicator</td><td data-bbox="1010 613 1908 695">Adjust the slider control to set the thresholds (% of compliant agents) for different alert levels.</td></tr> </table> <p data-bbox="667 743 1822 816">4. In the Exception List, select custom tags or filters to exclude users or endpoints from compliance calculations.</p> <p data-bbox="730 865 1839 938">Note: The Exceptions list applies to all Apex Central users. You may only add or delete exceptions based on your permissions to modify the corresponding tags and filters.</p> <p data-bbox="730 979 1759 1011">For more information about creating tags or filters, see Custom Tags and Filters.</p> <ol style="list-style-type: none"> <li data-bbox="806 1060 1440 1092">a. Click Add. The Add Exception screen appears. <li data-bbox="806 1141 1864 1214">b. From the Type drop-down list, <u>select User or Endpoint to display the available custom filters and tags by type</u>; otherwise, select All to view all entries. <p data-bbox="856 1263 1894 1336">Note: To search for a custom filter or tag, type a name in the text field and press ENTER.</p>	Column	Description	Acceptable pattern versions	Specify the pattern versions for endpoints to be considered compliant.	Alert indicator	Adjust the slider control to set the thresholds (% of compliant agents) for different alert levels.
Column	Description						
Acceptable pattern versions	Specify the pattern versions for endpoints to be considered compliant.						
Alert indicator	Adjust the slider control to set the thresholds (% of compliant agents) for different alert levels.						

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>For more information on custom tags and filters, see Custom Tags and Filters.</p> <p>c. Select one or more custom tags or filters and click Add. The selected items appear in the Exception List.</p> <p>d. Click Close.</p> <p>e. Click Save.</p> <p>f. Specify the scope of the added custom tags or filters from the Apply exceptions added by drop-down list.</p> <p>All user accounts: Excludes all users and endpoints specified in custom filters and tags added by any user account</p> <p>Only the logged on account: Excludes only the users and endpoints specified in custom filters and tags added by the currently logged on user account</p> <p>5. Click Save.”</p> <p>https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/getting-started/active-directory-and-001/compliance-indicator-001/configuring-the-anti.aspx</p> <p>“Data Loss Prevention</p> <p>Data Loss Prevention (DLP) safeguards an organization's confidential and sensitive data-referred to as digital assets-against accidental disclosure and intentional theft. DLP allows you to:</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<ul style="list-style-type: none"> • Identify the digital assets to protect • Create policies that limit or prevent the transmission of digital assets through common channels, such as email and external devices • Enforce compliance to established privacy standards <p>DLP evaluates data against a set of rules defined in policies. Policies determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission.”</p> <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 14-14 to 14-15 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>
<p>in response to administrator action, cause setting, before the second occurrence, of a second policy for the fourth instructions that is applied the group including each of the plurality of devices that has the at least one operating system installed thereon,</p>	<p>Trend Micro Apex Central infringes claim 1 and is configured to, <i>in response to administrator action</i> (e.g., user input, etc.), <i>cause setting, before the second occurrence</i> (e.g., the second discrete event that triggers at least one of the signature/policy updates for the intrusion prevention rules, etc.), <i>of a second policy</i> (e.g., a security policy designed for use in enforcing intrusion detection rule compliance, etc.) <i>for the fourth instructions that is applied the group including each of the plurality of devices</i> (e.g., managed products and endpoints, etc.) <i>that has the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>installed thereon</i>,</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: As set forth below, a security policy is capable of being set for use in enforcing intrusion detection rule compliance.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>“Each managed product provides <i>different policy settings</i> that you can <i>configure</i> and deploy to policy targets.”</p> <p>https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/policies/policy-management_001/policy-management_002/creating-a-new-polic.aspx (emphasis added)</p> <p>“Intrusion Prevention Rules</p> <p>The Intrusion Prevention Rules screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.</p> <ul style="list-style-type: none"> • To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule.” <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p> <p>“Endpoint Sensor</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>Endpoint Sensor is a powerful monitoring and investigation tool used to identify the presence, location, and entry point of threats. Through the use of detailed system event recording and historical analysis, you can perform preliminary investigations to discover hidden threats throughout your network and locate all affected endpoints. Generate root cause analysis reports to understand the nature and activity of the malware since the threat entered the endpoint.</p> <p>You can also perform detailed investigations through the use of shared IOC files and YARA rules. <u>Detailed investigations conduct in-depth, live searches of endpoints to locate previously unidentified threats and possible Advanced Persistent Threat attacks.</u></p> <p>Configuring Endpoint Sensor Settings</p> <p>Important: The Endpoint Sensor feature requires special licensing and additional system requirements. Ensure that you have the correct license before deploying Endpoint Sensor policies to endpoints. For more information on how to obtain licenses, contact your support provider.</p> <p>Procedure</p> <ol style="list-style-type: none"> 1. Select Enable Endpoint Sensor. 2. Select Enable event recording to begin collecting system event logs on the agent endpoint. <p><u>Endpoint Sensor uses the real-time event logs to identify at-risk endpoints when performing investigations. After identifying affected Windows endpoints, you can perform an in-depth root cause analysis to better understand possible attack vectors."</u></p> <p><i>Trend Micro Apex Central Widget and Policy Management Guide, Version: 2019, Page 14-2</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_wpg.pdf)</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p data-bbox="661 378 961 410">“Creating a New Policy</p> <p data-bbox="661 459 1896 570">Important: Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the <i>Apex Central Widget and Policy Management Guide</i>.</p> <ol data-bbox="661 618 1864 1166" style="list-style-type: none"> <li data-bbox="661 618 1724 651">1. Go to Policies > Policy Management. The Policy Management screen appears. <li data-bbox="661 699 1854 768">2. Select the type of product settings from the Product list. The screen refreshes to display policies created for the selected managed product. <p data-bbox="711 816 1881 885">For more information about configuring policy settings for specific managed products, see the <i>Apex Central Widget and Policy Management Guide</i>.</p> <ol data-bbox="661 933 1864 1166" style="list-style-type: none"> <li data-bbox="661 933 1318 966">3. Click Create. The Create Policy screen appears. <li data-bbox="661 1015 972 1047">4. Type a policy name. <li data-bbox="661 1096 1864 1166">5. Specify targets. Apex Central provides several target selection methods that affect how a policy works. <p data-bbox="711 1214 1539 1247">The policy list arranges the policy targets in the following order:</p> <ul data-bbox="760 1295 1923 1364" style="list-style-type: none"> <li data-bbox="760 1295 1923 1364">• Specify Targets: Use this option to select specific endpoints or managed products. For details, see Specifying Policy Targets.

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<ul style="list-style-type: none"> • Filter by Criteria: Use this option to allocate endpoints automatically based on the filtering criteria. For details, see Filtering by Criteria. • None (Draft only): Use this option to save the policy as a draft without choosing any targets. <p>For more information about the policy list, see Understanding the Policy List.</p> <p>6. Click a managed product feature to expand it and configure its settings. Repeat this step to configure all features.</p> <ul style="list-style-type: none"> • Each feature has a link to a Help topic that discusses the feature and how to use it. • For certain product settings, Apex Central needs to obtain specific setting options from the managed products. If administrators select multiple targets for a policy, Apex Central can only obtain the setting options from the first selected target. To ensure a successful policy deployment, make sure the product settings are synchronized across the targets. • If you are creating a policy for Apex One Security Agent that you want to act as a parent to a future child policy, configure settings that can be inherited, customized, or extended on the child policy. • For a list of Security Agent settings that can be inherited, customized, or extended, see Working with Parent Policy Settings. • For details on creating a child policy, see Inheriting Policy Settings.

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>7. Click Deploy or Save. If you clicked Deploy, Apex Central starts the deployment. The deployed policy appears in the list on the Policy Management screen. It usually takes a few minutes for Apex Central to deploy the policy to the targets.</p> <p>Click Refresh on the Policy Management screen to update the status information in the policy list. If the status of the deployment remains pending after an extended period of time, there might be issues with the targets. Check if there is a connection between Apex Central and the targets. Also check if the targets are working properly.</p> <p>Once Apex Central deploys a policy to the targets, the settings defined in the policy overwrite the existing settings in the targets. Apex Central enforces the policy settings in the targets every 24 hours. Although local administrators can make changes to the settings from the managed product console, the changes are overwritten every time Apex Central enforces the policy settings.</p> <ul style="list-style-type: none"> • Apex Central enforces the policy settings on the targets every 24 hours. Since policy enforcement only occurs every 24 hours, the product settings in the targets may not align with the policy settings if local administrators make changes through the managed product console between the enforcement period. • Policy settings deployed to IMSVA servers take priority over the existing settings on the target servers instead of overwriting them. IMSVA servers save these policy settings on the top of the list. • If an Apex One Security Agent assigned with a Apex Central policy has been moved to another Apex One domain, the agent settings will temporarily change to the ones defined

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>by that Apex One domain. Once Apex Central enforces the policy again, the agent settings will comply with the policy settings.”</p> <p>https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/policies/policy-management_001/policy-management_002/creating-a-new-polic.aspx</p>
<p>in response to administrator action, cause setting, before the third occurrence, of a third policy for the fifth instructions that is applied to the group including each of the plurality of devices that has the at least one operating system installed thereon, and</p>	<p>Trend Micro Apex Central infringes claim 1 and is configured to, <i>in response to administrator action</i> (e.g., user input, etc.), <i>cause setting, before the third occurrence</i> (e.g., the third discrete event that triggers at least one of the signature/policy updates for the firewall violation software, etc.), <i>of a third policy</i> (e.g., a security policy designed for use in enforcing prevent firewall compliance, etc.) <i>for the fifth instructions that is applied to the group including each of the plurality of devices</i> (e.g., managed products and endpoints, etc.) <i>that has the at least one operating system</i> (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) <i>installed thereon, and</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Note: As set forth below, a security policy is capable of being set for use in enforcing firewall compliance.</p> <p>“Each managed product provides <i>different policy settings</i> that you can <i>configure</i> and deploy to policy targets.”</p> <p>https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/policies/policy-management_001/policy-management_002/creating-a-new-polic.aspx (emphasis added)</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability		
	<p data-bbox="661 337 1289 370">“Configuring Additional Security Agent Services</p> <p data-bbox="661 418 800 451">Procedure</p> <ol data-bbox="661 500 1898 568" style="list-style-type: none"> <li data-bbox="661 500 1898 568">1. <u>Select to enable the required service on Windows desktops or Windows Server platforms in the following sections:</u> <ul data-bbox="661 617 1871 847" style="list-style-type: none"> <li data-bbox="661 617 1871 769">• Unauthorized Change Prevention Service <ul data-bbox="716 659 1871 769" style="list-style-type: none"> <li data-bbox="716 659 1871 769">○ For Windows Server platforms, select Only enable services required by Security Agent Self-protection features to ensure that the Security Agent program stays protected without affecting server performance. <li data-bbox="661 782 737 807">• ... <li data-bbox="661 816 921 847">• <u>Firewall Service</u> <p data-bbox="716 896 1856 1006"><u>Important:</u> Enabling or disabling the service temporarily disconnects endpoints from the network. Ensure that you change the settings only during non-critical hours to minimize connection disruptions.</p> <ul data-bbox="661 1055 1113 1123" style="list-style-type: none"> <li data-bbox="661 1055 1113 1086">• Suspicious Connection Service <li data-bbox="661 1096 1024 1123">• Data Protection Service <p data-bbox="661 1136 699 1161">...”</p> <p data-bbox="661 1174 1814 1247"><i>Trend Micro Apex Central Widget and Policy Management Guide, Version: 2019, Page 6-3</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_wpg.pdf</p> <table data-bbox="661 1289 1906 1326"> <tr> <td data-bbox="661 1289 1010 1326">Section</td><td data-bbox="1010 1289 1906 1326">Settings</td></tr> </table>	Section	Settings
Section	Settings		

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Firewall	<ul style="list-style-type: none"> • Display the Firewall settings on the Security Agent console: Allows users to configure the Firewall settings on the Security Agent console • Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message: Displays the Enable/Disable Firewall and Enable/Disable IDS Mode menu options on the Security Agent system tray icon <p>Note: The Apex One Firewall protects agents and servers on the network using stateful inspection, high performance network virus scanning, and elimination. If you grant users the privilege to enable or disable the firewall and its features, warn them not to disable the firewall for an extended period of time to avoid exposing the endpoint to intrusions and hacker attacks.</p> <ul style="list-style-type: none"> • Allow Security Agents to send firewall logs to the Apex One server: Configures the Security Agent to send Firewall logs to the server, allowing you to analyze network traffic
	<p><i>Trend Micro Apex Central Widget and Policy Management Guide, Version: 2019, Page 6-6</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_wpg.pdf</p> <p>“Adding a Firewall Policy</p> <p>1. Go to Agents > Firewall > Policies.</p>	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>2. Select to add, copy, or modify a policy.</p> <ul style="list-style-type: none"> Click Add to create a new policy. Select an existing policy and click Copy to open the Copy Policy screen. Modify the policy settings as required. Click the Policy Description of an existing policy to modify settings. <p>3. In the Firewall Policy section, configure the following:</p> <ul style="list-style-type: none"> Name: Specify a unique name for the Apex One Firewall policy. Security level: Select from High, Medium, or Low to determine the type of traffic that the Apex One Firewall allows or blocks. <p>Note: The Apex One Firewall automatically allows or blocks connections through the ports specified in the Exception Template list.</p> <p>For more information, see Editing the Apex One Firewall Exception Template List.</p> <p>4. In the Firewall Features section, configure the following:</p> <ul style="list-style-type: none"> Enable firewall: Select to activate the Apex One Firewall for this policy. Enable Intrusion Detection System (IDS): Select to attempt and identify patterns in network patterns that may indicate an attack.

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>For more information, see Intrusion Detection System.</p> <ul style="list-style-type: none"> • Display a notification when a Firewall violation is detected: Select to display a notification on the Security Agent when the Apex One Firewall blocks an outgoing packet. <p>Important: If you grant users the permission to configure Apex One Firewall settings using the Security Agent console, you cannot use the Apex One web console to override the settings that the user configures.</p> <p>The information under Settings on the Security Agent console's Firewall tab always reflects the settings configured from the Security Agent console, not from the server web console.</p> <p>5. In the Certified Safe Software List section, configure the following:</p> <ul style="list-style-type: none"> • Enable the local Certified Safe Software List: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. ○ Enable the global Certified Safe Software List (Internet access required): Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. <p>Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability		
	<p>6. In the Exception section, manage the Exception Template List that applies to this policy only. The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.</p> <p>For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3).</p> <p>7. Click Save."</p> <p>https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)</p>		
<p>cause the utilization of the different occurrence mitigation actions of the diverse occurrence mitigation types, including the firewall-based occurrence mitigation type and the other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing the advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse</p>	<p>Trend Micro Apex Central infringes claim 1 and is configured to <i>cause the utilization of the different occurrence mitigation actions of the diverse occurrence mitigation types, including the firewall-based occurrence mitigation type (e.g., firewall configuration, etc.) and the other occurrence mitigation type (e.g., intrusion detection, etc.), across the plurality of devices (e.g., managed products and endpoints, etc.) for occurrence mitigation by preventing the advantage being taken of the actual vulnerabilities (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices (e.g., managed products and endpoints, etc.)</i>.</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <table border="1" data-bbox="661 1328 1911 1369"> <tr> <th data-bbox="661 1328 1012 1369">Consideration</th><th data-bbox="1012 1328 1911 1369">Effect</th></tr> </table>	Consideration	Effect
Consideration	Effect		

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
occurrence mitigation types across the plurality of devices.	Deployment planning	Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to <u>products based on Deployment Plans</u> . These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.
	Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)	
	“Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system	
	...	
	Table 1. Product Status Information Data View	
	Operating System	The operating system on the managed product server or Security Agent endpoint
	OS Version	The version of the operating system on the managed product server or Security Agent endpoint
	OS Service Pack	The service pack number of the operating system on the managed product server or Security Agent endpoint
	Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability
	<p>“ ...</p> <p>5. In the Certified Safe Software List section, configure the following:</p> <ul style="list-style-type: none"> • Enable the local Certified Safe Software List: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. • Enable the global Certified Safe Software List (Internet access required): Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. <p>Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.</p> <p>6. In the Exception section, manage the Exception Template List that applies to this policy only. <u>The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.</u></p> <p>For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3).</p> <p>7. Click Save.”</p> <p>https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)</p> <p>“Detailed Firewall Violation Information</p>

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability																				
	Provides <u>specific firewall configuration information on your network</u> , such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations”																				
	<table> <tr> <th>Section</th><th>Settings</th></tr> <tr> <td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr> <tr> <td>Generated</td><td>The date and time the managed product generated the data</td></tr> <tr> <td>Product Entity/Endpoint</td><td>Depending on the related source: <ul style="list-style-type: none"> The display name of the managed product server in Apex Central The name or IP address of the endpoint Product </td></tr> <tr> <td>Product</td><td>The name of the managed product or service Example: Apex One, ScanMail for Microsoft Exchange</td></tr> <tr> <td>Event Type</td><td>The type of event that triggered the detection Example: intrusion, policy violation</td></tr> <tr> <td>Risk Level</td><td>The Trend Micro assessment of risk to your network Example: High security, low security, medium security</td></tr> <tr> <td>Traffic/Connection</td><td>The direction of the transmission</td></tr> <tr> <td>Protocol</td><td>The protocol the intrusion uses Example: HTTP, SMTP, FTP</td></tr> <tr> <td>Source IP</td><td>The source IP address of the detected threat</td></tr> </table>	Section	Settings	Received	The date and time Apex Central received the data from the managed product	Generated	The date and time the managed product generated the data	Product Entity/Endpoint	Depending on the related source: <ul style="list-style-type: none"> The display name of the managed product server in Apex Central The name or IP address of the endpoint Product 	Product	The name of the managed product or service Example: Apex One, ScanMail for Microsoft Exchange	Event Type	The type of event that triggered the detection Example: intrusion, policy violation	Risk Level	The Trend Micro assessment of risk to your network Example: High security, low security, medium security	Traffic/Connection	The direction of the transmission	Protocol	The protocol the intrusion uses Example: HTTP, SMTP, FTP	Source IP	The source IP address of the detected threat
Section	Settings																				
Received	The date and time Apex Central received the data from the managed product																				
Generated	The date and time the managed product generated the data																				
Product Entity/Endpoint	Depending on the related source: <ul style="list-style-type: none"> The display name of the managed product server in Apex Central The name or IP address of the endpoint Product 																				
Product	The name of the managed product or service Example: Apex One, ScanMail for Microsoft Exchange																				
Event Type	The type of event that triggered the detection Example: intrusion, policy violation																				
Risk Level	The Trend Micro assessment of risk to your network Example: High security, low security, medium security																				
Traffic/Connection	The direction of the transmission																				
Protocol	The protocol the intrusion uses Example: HTTP, SMTP, FTP																				
Source IP	The source IP address of the detected threat																				

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Endpoint Port	The port number of the endpoint under attack
	Endpoint IP	The IP address of the endpoint
	Target Application	The application the intrusion targeted
	Description	The detailed description of the incident by Trend Micro
	Action	The action taken by the managed product Example: file cleaned, file quarantined, file passed
	Detections	The total number of detections Example: A managed product detects 10 violation instances of the same type on one computer Detections = 10
	Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)	
	Feature	Description

	Vulnerability Protection Integration	Integration with Vulnerability Protection protects Apex One users by <u>automating the application of virtual patches before official patches become available</u> . Trend Micro provides protected endpoints with <u>recommended Intrusion Prevention</u> rules based on your network performance and security priorities.

	https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx	

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability						
	<p>“Intrusion Prevention Rules</p> <p>The Intrusion Prevention Rules screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.</p> <ul style="list-style-type: none"> • To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns. • To sort the list of Intrusion Prevention Rules by column data, click a column heading. • To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule.” <p><i>Trend Micro Apex Central Administrator’s Guide</i>, Version: 2019, Page 14-33 https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf</p> <p>“The Threat Type column displays the following threat types.</p> <table border="1"> <thead> <tr> <th>Threat Type</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Ransomware</td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr> <tr> <td><u>Known Advanced Persistent Threat (APT)</u></td><td><u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u></td></tr> </tbody> </table>	Threat Type	Description	Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid	<u>Known Advanced Persistent Threat (APT)</u>	<u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u>
Threat Type	Description						
Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid						
<u>Known Advanced Persistent Threat (APT)</u>	<u>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u>						

PRELIMINARY CLAIM CHART

Patent No. 10,893,066, Claims 1 and 2: Trend Micro Apex Central

Claim 2 Elements	Applicability	
	Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file
	Vulnerability attack	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems
	Lateral movement	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
	Unknown threats	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer
	C&C callback	Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware
<i>Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20</i> https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf		

Caveat: The notes and/or cited excerpts utilized herein are set forth for illustrative purposes only and are not meant to be limiting in any manner. For example, the notes and/or cited excerpts, may or may not be supplemented or substituted with different excerpt(s) of the relevant reference(s), as appropriate. Further, to the extent any error(s) and/or omission(s) exist herein, all rights are reserved to correct the same in connection with any subsequent correlations.